UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

JON KAHEN, a/k/a JON KAEN, GLOBAL VOICECOM, INC., GLOBAL TELECOMMUNICATION SERVICES INC., and KAT TELECOM, INC.,

Defendants.

Civil Action No.

CV 20-00474

COGAN, J.

DECLARATION OF SEAN FAGAN

I, Sean Fagan, have personal knowledge of the facts set forth below, and if called as a witness I would testify as follows:

1. I have been a Special Agent with the Social Security Administration's Office of the Inspector General ("SSA OIG") since September 2017. As an SSA OIG Special Agent, I investigate threats against Social Security employees and facilities, employee malfeasance, and Social Security fraud, such as direct deposit fraud, identity theft, social security number misuse, and other types of fraud against Social Security programs. I have six years of prior federal law enforcement experience as a Special Agent with the Diplomatic Security Service under the U.S. Department of State, where both domestically and internationally I investigated crimes such as passport fraud, visa fraud, identity theft, employee malfeasance, and threats and other crimes involving U.S. Government personnel, property, and information. In 2011, I completed the Federal Law Enforcement Training Center's Criminal Investigator Training Program, a comprehensive 11-week course that included training in electronic sources of information,

conducting investigations in a cyber environment, and financial aspects of investigations. I then completed the Diplomatic Security Service's Basic Special Agent Course that included an additional 12 weeks of training in topics such as dignitary protection, visa and passport fraud investigations, and international investigations. I have completed advanced training on topics such as financial record analysis, cellphone record analysis, and internet investigations. Further, over the course of my federal law enforcement career, I have worked with and received guidance from other experienced investigators from various federal, state, local, and foreign law enforcement agencies in the fields of general crimes, fraud, identity theft, financial crimes, digital crimes, dignitary protection, kidnapping/hostage-taking, counterintelligence, and terrorism. Prior to beginning my federal law enforcement career, I served in the U.S. Marine Corps for 10 years as an infantryman and counterintelligence/human intelligence officer. I also hold a Bachelor of Science in criminal justice.

2. During my law enforcement career, I have conducted arrests, search warrants, and physical surveillance. I have prepared affidavits to support the establishment of probable cause for search and arrest warrants. I am familiar with the facts set forth below based upon my own investigative findings and conversations with other participating law enforcement agents and private sector investigators.

3. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, information from other individuals including other law enforcement officers, complainants, and other parties, witness interviews, and my review of documents, public records, SSA records, and other sources. Because this declaration is submitted for the limited purpose of establishing probable cause in support of the application

for a temporary restraining order, it does not set forth each and every fact that I and other investigators have learned during the course of this investigation.

4. SSA imposter fraud has resulted in the filing of hundreds of thousands of complaints with the Administration in just the last fifteen months. Specifically, analysis of our complaints database reveals 465,843 complaints about fraudulent telephone impersonation of the Administration between October 1, 2018 and September 30, 2019; these complaints reflect aggregated losses of $14,486,453.64.

5. In addition, the Federal Trade Commission ("FTC") collects complaints in its Consumer Sentinel database on SSA and other government-imposter scams. For 2018, the FTC received 39,427 fraud complaints about SSA imposters, which related losses of $11,589,466. SSA imposter fraud complaints for 2019 include 166,190 complaints relating $37,815,433 in losses. The FTC received even more complaints regarding government-imposter frauds in general, which include SSA imposter frauds; this broader category contains 255,223 complaints reflecting $128,479,054 in losses for 2018, and 389,563 complaints reflecting $152,946,623 in losses for 2019. In my experience, these complaint numbers substantially underrepresent the extent of fraudulent activity, because most victims do not report their losses to the government.

6. The FTC also collects do-not-call ("DNC") complaints. The Consumer Sentinel database reflects 12,372 DNC complaints about SSA imposter robocalls for 2018, and 179,537 complaints about SSA imposter robocalls for 2019, more than a tenfold increase. Regarding government, business, and other categories of imposter robocalls generally, the Consumer Sentinel database contains 334,044 DNC complaints for 2018, and 566,263 for 2019.

OVERVIEW OF DEFENDANTS' WIRE FRAUD SCHEMES

7. This investigation involves wire fraud schemes conducted and facilitated by Jon Kahen, a/k/a Jon Kaen ("Kaen") through the entities Global Voicecom, Inc., Global Telecommunication Services Inc., and KAT Telecom, Inc. Kaen also conducts telecommunications business under the name IP Dish. Kaen resides in Great Neck, New York, and operates and controls the named entities from his home.

8. As relevant to this Declaration, "robocalling" refers to an automated process of placing large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person. SSA OIG is investigating criminal schemes perpetrated by individuals operating one or more call centers located in India and other foreign locations. Fraudsters at the call centers impersonate government agencies and other entities—including the SSA, other government agencies, and businesses—and place millions of robocalls to phones in the United States. These robocalls convey recorded messages instructing the recipients to contact the impersonated entity regarding problems with their social security numbers, missed court dates, imminent asset freezes, or other such lies that are intended to scare the recipient into establishing phone contact with a criminal. In all of these schemes, the criminals attempt to defraud and extort money from anyone who contacts them in response to their messages.

9. Since at least 2017, Kaen and the companies he operates have knowingly provided robocall fraudsters with unfettered access to the U.S. phone system and thus the ability to deluge U.S. telephones with millions of fraudulent robocalls. Kaen and these entities have also provided fraudsters with hundreds of phone numbers and toll-free phone numbers used in furtherance of the robocall fraud schemes, to allow victims to return calls to the fraudsters in foreign locations at

what appear to the potential victims to be legitimate U.S. phone numbers and toll-free numbers, further cloaking the frauds in facades of legitimacy.

10. In furtherance of the fraudulent schemes, Kaen has also received at least one direct payment from a victim of one of the fraudulent schemes.

11. Kaen's participation in these fraudulent robocall schemes is essential to the schemes' success. Without someone willing to accept the fraudsters' robocall traffic into the U.S. telephone system, even though the fraudsters have internet access they would be unable to contact any potential victims in the first instance. That is because Kaen provides the crucial interface between foreign internet-based phone traffic and the U.S. telephone system, and our investigation reveals that he does so with full knowledge that he is facilitating massive frauds. Similarly, by providing internet-based return-calling and toll-free services, Kaen not only enables initial contact with potential victims, but also allows the unwitting to become victims when they return calls to fraudsters after they receive a fraudulent robocall voicemail message.

12. The robocall imposters in this investigation use a variety of methods to receive funds from victims, including but not limited to asking victims to: purchase gift cards or other stored value cards and then to transmit the numbers from the back of the cards to the fraudsters; to send bank wires; and to send cash payments by overnight carrier.

13. In the course of this investigation, we learned that Defendants have transmitted calls as part of numerous fraudulent robocalling schemes, including:

a. *SSA Imposters*: SSA imposters send recorded messages falsely claiming that the recipient's social security number has been used in criminal activity, the recipient's social security benefits will be suspended, the recipient failed to appear before a grand jury and faces imminent arrest, or the recipient's social security number will be terminated.

When an individual calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until the individual is issued a new social security number, at which point the individual's funds will be returned.

b. *Internal Revenue Service ("IRS") and Treasury Imposters*: IRS imposters send recorded messages falsely claiming that the recipient has been implicated in tax fraud, the individual has avoided attempts to enforce criminal laws, the individual has avoided court appearances, or the individual faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically tells the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.

c. *United States Citizenship and Immigration Services ("USCIS") Imposters*: USCIS imposters send recorded messages falsely claiming that the recipient failed to fill out immigration forms correctly, the recipient faces imminent arrest or deportation, that the recipient's home country has taken formal action against the recipient that may result in deportation, or the recipient has transferred money in a way that will result in deportation. When a recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the recipient to pay various fees or fines to avoid immigration consequences.

d. *Foreign Government Imposters*: Foreign government imposters send recorded messages, often in foreign languages, falsely claiming to be from the U.S.-based consulate of a foreign government and claiming that the recipient has been implicated in criminal activity. When recipients call back or connects to the fraudster, the fraudster

falsely claims that the recipient must pay various fees or fines in order to avoid immigration consequences, such as deportation and criminal sanctions.

e. *Tech Support Imposters*: Fraudsters operating tech support scams impersonate various well-known tech companies, such as Apple or Microsoft, and send recorded messages falsely claiming that the recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster often convinces the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

TECHNOLOGIES USED IN THE FRAUDULENT ROBOCALLING SCHEMES

14. The technical ability to place the fraudulent robocalls at issue in the investigation is dependent on (1) voice-over-internet-protocol (VoIP) and related technology to create the calls, and (2) a "gateway carrier" to introduce the foreign phone traffic into the U.S. phone system. In the telecommunications industry, the term "gateway carrier" refers to a U.S.-based person or entity that agrees with a foreign person or entity (often by contract) to accept foreign-source VoIP telephone traffic into the U.S. telephone system, to pass that telephone traffic to other U.S.-based carriers, and thus route the calls to their ultimate destination in the United States. VoIP uses a broadband internet connection—as opposed to an analog copper phone line—to place phone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional, wired phone. The technology employed by modern telecommunication providers mediates between digital VoIP signals and regular telephone signals so that communication is seamless between VoIP and non-VoIP users at either end. VoIP is used

in the schemes both to place robocalls to U.S. phones and to communicate with individuals who either answer the robocall or call the number contained in the recorded robocall message.

15. VoIP relies upon a set of rules for electronic communication called Session Initiation Protocol ("SIP"). Much like the way browsing websites on the internet uses HyperText Transfer Protocol ("HTTP") to initiate and conduct information exchanges between devices through exchanges of packets of information, SIP is a set of rules used to initiate and terminate live sessions for things such as voice and video communication between two or more points connected to the internet. Both SIP voice communication and HTTP web-browsing rely on exchanging data packets between two points. For example, web browsing via HTTP requires an individual to request information from another point on the internet, usually by clicking on a hyperlink or entering a web address in a browser's address bar, usually preceded by "http://www," which tells the device that it is making a request for information on the World Wide Web via HTTP. A device receiving that request will send back information to the requesting device, and thus, the requesting device will display the requested website.

16. Similarly, a voice call via SIP starts as a data packet sent to initiate a call, a responsive packet sent back that indicates whether the call has been answered, and numerous other packets transiting back and forth; amongst these data packets is information that machines turn into audible signals, i.e., a conversation that can be heard by the participants. In the case of robocalls, a recorded message is transmitted once the call is answered by voicemail picking up or a live person answering.

17. Robocalls should not be understood as traditional telephone calls, but rather, requests for information and responsive data packets transiting the internet via SIP. An outgoing robocall begins as a request for information sent by an automatic telephone dialing system known

as an "autodialer" that—in conjunction with VoIP services—enables the caller to make millions of sequential requests for information (i.e., outbound VoIP phone calls) in a very short time. A VoIP autodialer is a specialized type of telecommunications equipment with the capacity to (1) store or produce telephone numbers to be called, and (2) request responsive information from devices at the other end of the call, i.e., dial the telephone numbers. The autodialer's requests for information are directed to devices (here, telephones) that send back responsive information when the call is answered either by a live person or the person's voicemail. When the autodialer receives information from the called device indicating that the call is answered, the autodialer will then send information back to that device (the phone) in the form of a recorded message. As relevant here, fraudsters created the recorded message that conveys false threats while impersonating a U.S. government agency or the other entities described above.

18. A fraudster making these robocalls can not only send a recorded message to the individual's phone, but can misrepresent who is calling on the caller ID. Normally, a recipient's caller ID will display information identifying the caller by means of a telephone number that is automatically displayed because the caller owns the right to use that phone number; however, many VoIP software packages allow the caller to specify the information appearing on the call recipient's caller ID, much in the same way an email's subject line can be edited to state whatever the sender wishes. This practice of specifying what appears on the recipient's caller ID is called "spoofing." This feature of VoIP technology permits a caller with an illicit motive to spoof a legitimate phone number, such as that belonging to a government entity, in order to cloak the fraudsters with indicia of authority and induce the recipients to answer the call. Spoofing also encourages potential victims to return calls when they look up the spoofed number and see that it

is a number used by an official government entity. In these robocalling schemes, spoofing serves the purpose of deceiving the potential victim about who is calling them.

19. Spoofing any phone number is a simple matter of editing a SIP file to state the desired representation on the caller ID. These files can then be loaded into an autodialer to become robocalls, replicated millions of times with the spoofed, fraudulent caller ID information.

20. The fraudulent robocalls generally leave prerecorded, threatening messages for recipients. Some of the fraudulent messages direct the recipient to press a key to speak with a live operator. Other fraudulent messages leave a domestic telephone number as a "call-back" number. In either case, whether the recipient presses a key or calls the call-back number, the recipient will be connected to a fraudster in a foreign call center.

21. A gateway carrier is an essential element of the fraud schemes perpetrated through these robocall schemes. Foreign calls centers and VoIP providers cannot connect VoIP phone traffic directly to the U.S. telephone system from a foreign location without the assistance of a U.S.-based telecommunications provider willing to accept the foreign traffic. For example, a fraudulent call center in India cannot directly upload tens of millions of robocalls to the U.S. telephone system, even where they have broadband internet and VoIP service. Foreign VoIP telephone traffic cannot enter the U.S. telephone system without travelling through a gateway carrier willing to accept the foreign traffic and introduce it to the U.S. telephone system. Global Voicecom serves as a carrier for calls originating abroad and that are bound for the United States. Global Voicecom states on its website that its "ever-expanding portfolio of services includes . . . US and international voice termination," meaning that it carries calls from overseas and passes them into the U.S. telephone system, and will pass calls from the United States to overseas. For many, if not all of the robocalls for which Global Voicecom provides terminations services, it is a

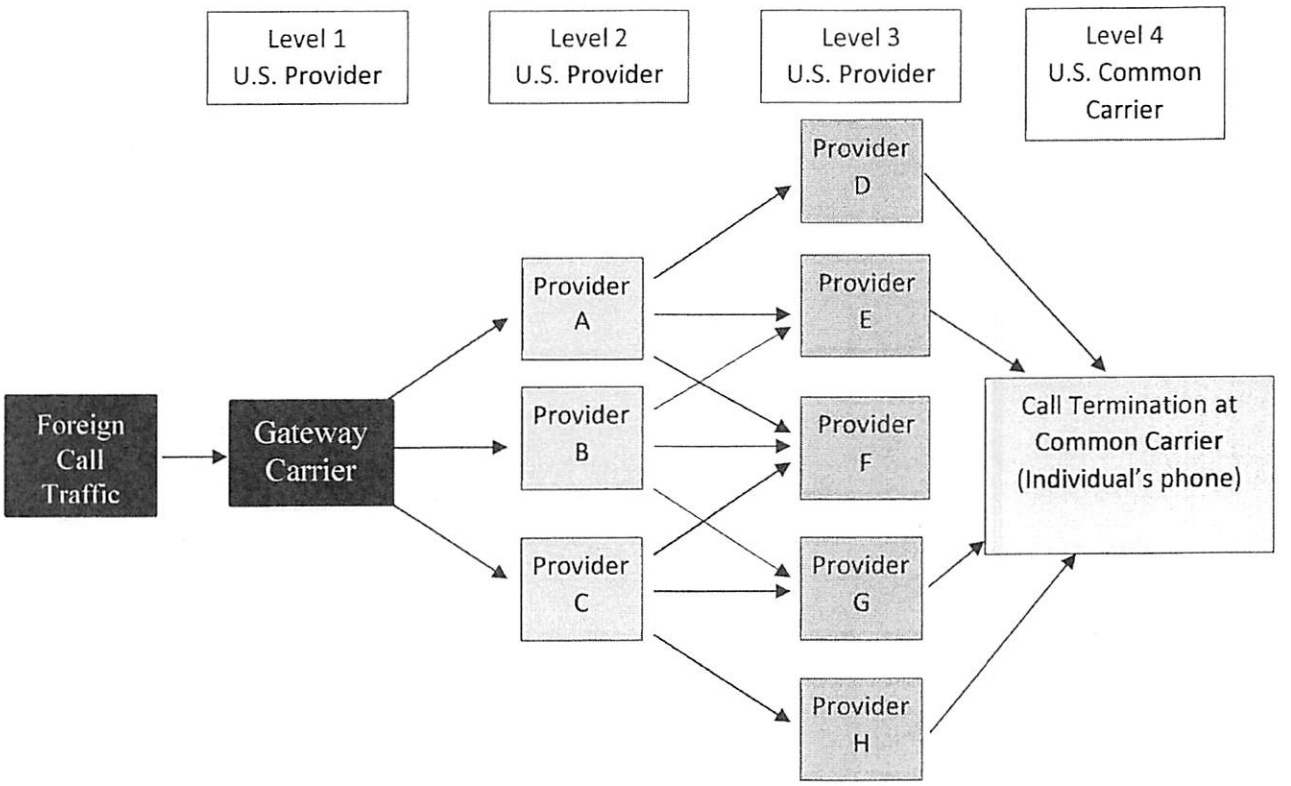
gateway carrier. In the context of the schemes, U.S.-bound fraudulent robocalls are "US terminat[ed]" calls, and return calls to fraudsters in other countries are "international voice terminat[ed]" calls.

22. In the course of this investigation, I learned that with little more than off-the-shelf VoIP technology, an autodialer, and a gateway carrier, any individual or entity with a broadband internet connection can introduce unlimited numbers of robocalls into the U.S. telephone system from any location in the world.

LEAST-COST CALL ROUTING AND TRACEBACKS

23. When foreign call centers route fraudulent robocalls through Defendants to recipients in the United States through VoIP technology, the calls typically pass through many different VoIP carriers. First, the calls typically pass from a foreign VoIP carrier to Defendants as the U.S. gateway carrier. From Defendants, calls typically pass through multiple other carriers until they reach a common carrier such as AT&T or Verizon. Consumer-facing companies like Verizon and AT&T are known in the industry as "common carriers."

24. With modern telecommunications infrastructure, outbound VoIP calls do not take a defined path from their origin to the final destination. Rather, the systems route calls through automated equipment that determines the lowest possible connection cost at each routing step, depending on preexisting contractual relationships between the various entities. Typically, companies at each routing step will have numerous existing contracts through which it can route outbound calls through intermediate providers to the common carriers as the last routing step before a U.S. individual can answer the call. This automated routing process is called "least-cost routing," illustrated in the following diagram beginning with a first-level U.S. gateway carrier:



In this simple example, arrows represent possible routing paths between providers based on preexisting contracts. Here, the gateway carrier has three contracts with second-level U.S. providers A, B, and C, each of which in turn has three contracts with third-level providers further into the U.S. phone system (denoted by Providers D, E, F, G, and H). Each of the third-level providers is able to pass calls to the fourth-level common carrier that provides telephone service to the U.S. individual. Which specific path a call takes is dependent on the effective contract terms between the gateway carrier, providers, and common carriers at the time the call is routed that achieve the lowest cost to transmit the call, i.e., "least-cost routing." In real-world application, least-cost routing may involve more than four levels of U.S. companies.

25. In light of least-cost routing and the prevalence of spoofing telephone numbers, identifying the source of any specific robocall requires a labor-intensive process known in the

telecommunications industry as "traceback." In order to conduct the traceback, an investigator must trace backwards each individual "hop" the call took in its least-cost-routing journey from the gateway carrier. For example and referencing the diagram above, the common carrier will be able to query its own system and determine which Level 3 Provider it received the call from, but it will not be able to see beyond that. The common carrier must contact the Level 3 Provider and ask that carrier to determine from its records what Level 2 Provider it received the call from. The common carrier must then contact the Level 2 Provider and ask them to determine which Level 1 provider they received the call from. This process continues at each "hop" until a provider identifies a foreign source—that carrier is then the "gateway carrier" that permitted the foreign telephone traffic to enter the U.S. phone system.

DIRECT-INWARD-DIAL NUMBERS AND TRACE-FORWARD

26. The schemes facilitated by the Defendants also rely upon the use of VoIP technology to receive inbound calls from U.S. individuals. Such inbound calling utilizes what is known in the telecommunications industry as direct-inward-dial ("DID") telephone numbers. DID numbers and the service associated with them can be purchased by an end-user.

27. DID numbers for inbound calling do not work the same way in the U.S. phone system as least-cost routing for outbound calling. The Federal Communications Commission ("FCC") provides phone numbers in large blocks to licensed telecommunication carriers. These numbers are used for numerous purposes in the telecommunications industry. As applicable here, DID numbers are used by a telecommunications company to provide inbound calling services to their customers. Such a customer may be an end-user of the DID number or may be another telecommunications provider who seeks to resell the inbound DID services to one of its customers.

The DID service (and the ability to use the DID number) can be resold any number of times by successive providers.

28. When a caller such as a U.S. individual places a call to a DID number, the individual's common carrier will route the call to the company that first obtained the DID number from the FCC. If that first company resold the number and its services, they will route it to the purchaser. This process continues until the call reaches the final seller in the chain, who will (in the case of VoIP calls) route the call to an IP address[1] on the internet designated by the end user of the DID number, who will then receive the call. Because the call is routed through these successive owners and must reach a specific location on the internet, the DID number cannot be spoofed.

29. There are no restrictions on how many times a DID number can be resold by successive providers. In order to determine the end-user of a DID telephone number, it is necessary to "trace forward" a call to the end-user of the DID number through the successive steps of purchasing and re-selling of that particular DID service. Unlike tracing an outbound robocall through the LCR process, tracing forward a DID phone number does not trace the record of an actual phone call in most cases, but rather, traces successive sales and ownership records of the right to use a phone number at a relevant point in time.

DEFENDANTS' KNOWLEDGE OF FRAUDULENT ROBOCALLS

30. Over a period of years, Defendants received many notices, inquires, warnings, complaints, and subpoenas concerning fraudulent robocalls and other suspect calls transiting their

[1] "IP address" means "Internet Protocol address." An IP address is a unique number assigned to a device connected to the internet.

systems, including such notices about fraudulent U.S.-bound robocalls, calls from U.S. individuals who were duped into returning messages to fraudsters on DID and toll-free telephone numbers provided by the Defendants, and specific victims' fraud losses. These warnings and inquiries came from other telecommunications companies, an industry trade group, and government bodies, the latter of which included not only general inquiries but also formal subpoenas for information about fraud. Nevertheless, Defendants continue to enable these massive fraud schemes to be perpetrated on U.S. individuals.

Inquiries, Complaints, and Notices from Other Telecommunication Companies

31. Analysis of records provided by Google, Paypal, the FCC, Verizon, and other sources demonstrate that the email address [XXXXXX]75@gmail.com is used by Kaen to conduct business on behalf of the fraudulent robocalling schemes and operate through the various corporate entities and IP Dish. Kaen also uses email addresses in the @globalvoicecom.com domain.

32. Peerless Network, Inc., another U.S. VoIP carrier, sent numerous notifications to Defendants and made requests for appropriate action concerning suspect calls transiting Defendants' network. For example, on September 11, 2018, Peerless emailed the [XXXXXX]75@gmail.com address and stated:

> We have received reports of possible spoofing calls to or from multiple numbers. From our queries we're seeing the calls ingress to us from your network. Please investigate and take the appropriate action.

Peerless included sample call information in furtherance of its request that Defendants investigate and act. Peerless sent similar emails to Defendants on: October 24, 2018; October 26, 2018; November 1, 2018; November 27, 2018; November 28, 2018; December 1, 2018; December 5, 2018; January 18, 2019; February 22, 2019; March 1, 2019; and March 5, 2019.

33. The U.S. common carrier AT&T has notified Defendants on numerous occasions about fraud traced to its operations. For example:

a. On November 16, 2017, AT&T sent an email to "IP DISH Team" at the [XXXXXX]75@gmail.com address:

> The following calls to AT&T cell phone customers were received using the spoofed caller ID numbers of a non-working number at the US Department of Homeland Security headquarters. Callers impersonated US Citizenship and Immigrations Services personnel and defrauded an AT&T customer of $1,450. . . .
> Pursuant to the customer and carrier network fraud protection provisions of the Telecommunication Act and the Telephone Records Privacy Protection Act (47 USC 222(d)(2)), could you provide the name(s) of your upstream carriers? We are tracing these calls to their source so they can be stopped.

AT&T sent similar emails about USCIS imposter robocalls to various email addresses in the globalvoicecom.com domain, including Kaen's email, on: September 11, 2017; November 29, 2017; April 30, 2018; and July 3, 2018.

b. On January 29, 2019, AT&T sent an email to "iVoice Team" at the [XXXXXX]75@gmail.com address:

> We have been receiving AT&T customers complaints about spoofing fraud from your network. In the first complaint calls are originating from a toll free number owned by the US Social Security Administration. Callers falsely claim to be US Government officials and attempt to extort money from our customers. We have verified this number is not out-pulsed as a legitimate caller ID by the real US Social Security Administration. . . .
> In the second complaint calls are originating from the toll free number of DirecTV (AT&T). Callers falsely claim to be AT&T/DirecTV technical reps and social engineer remote access to our customer's computers in order to make fraudulent wire transfers from online banking applications. . . .
> Could you provide the names and contact numbers of the parties that sent these calls to your network.

Records obtained in the course of this investigation demonstrate that more than 29,000 of these spoofed SSA calls originated from IP Dish on January 24, 2019 alone, which were associated with the email address [XXXXXX]75@gmail.com. According to AT&T, IP Dish did not respond to AT&T's email, although other records show that AT&T's email was received by the [XXXXXX]75@gmail.com email account. AT&T sent similar emails about SSA imposter robocalls to email addresses in the globalvoicecom.com domain, including Kaen's email address, on February 11, 2019 and May 2, 2019.

Defendants Knowingly Provide Return-Calling Services for the Fraudulent Schemes

34. AT&T also received a number of complaints about the telephone number 619-[XXX]-[XXXX] and fraudulent SSA imposter robocalls coming from that number. AT&T fraud investigators associated that phone number with data maintained by Nomorobo, a software application that blocks robocalls. According to Nomorobo, that phone number was associated with fraudulent robocalls containing the following message:

> Hello This call is from Department of Social Security Administration the reason you have received this phone call from our department is to inform you that there is a legal enforcement actions filed on your social security number for fraudulent activities so when you get this message kindly call back at the earliest possible on our number before we begin with the legal proceedings that is 619-[XXX]-[XXXX] I repeat 619-[XXX]-[XXXX] thank you.

A number of AT&T customers had placed calls to this number. AT&T investigators called this number several times and spoke to people who claimed to be from SSA. AT&T traced-forward this DID number to XO Communications, who informed AT&T that it was resold to Exiant Communications. Exiant Communications is closely affiliated with Blitz Telecom Consulting, LLC ("Blitz Telecom"), which resold the DID number to Global Voicecom.

35. Pursuant to an April 2016 contract, Blitz Telecom provided DID telephone numbers and associated services to Global Voicecom. Kaen signed the contract as the "Executive Director"

of Global Voicecom. Blitz Telecom and Exiant Communications have sent several dozen emails to Global Voicecom in 2017, 2018, and 2019, raising concerns about IRS imposter scams, SSA imposter scams, loan scams, tech support imposter scams, and other schemes using Global Voicecom's DID numbers. For example:

a. On September 13, 2017, Blitz Telecom emailed Global Voicecom as follows:

> The DID: 847[XXXXXXX] which we show assigned to you, is being used for fraudulent purposes. The US Treasury Department has provided us with a few complaints which are listed below. Because of the nature of the complaints, we have disabled this number on our network.
>
> I received a call from 484-[XXX]-[XXXX] claiming that I was a subject of Treasury Fraud. they said to call back at 847-[XXX]-[XXXX]. The call was received on Friday September 8th at 4 pm. I live in Philadelphia, in the EST zone. They claimed I would be sued if I did not call back.
>
> I received a voicemail message with an automated recording claiming to be from the US Dept. of Treasury regarding tax fraud in my name. The call back number was 847-[XXX]-[XXXX]. No one answered the return call. I recently submitted via mail my 3rd installment of 2017 taxes, so I hope nothing has gone wrong in the process of receiving my payment. Is this a known scam number? Thank you.
>
> The voice message states (Pre-recorded): "Treasury my badge number is 4874. The nature and purpose of this call is regarding an enforcement action which has been executed by the us treasury department regarding tax fraud against your name. Ignoring this would be an intentional attempt to avoid initial appearance before the majesty does or exempt or enforce criminal offence. Before this matter goes to federal claim, court house, or before you get arrested. Kindly call us back as soon as possible. The number to reach us is 847-[XXX]-[XXXX], let me repeat the number 847-[XXX]-[XXXX]. Hope to hear from you soon before the charges are pressed against you. Thank you."

b. On January 17, 2018, Blitz Telecom emailed Global Voicecom:

> We have received a complaint that the number 312[XXXXXXX] is being used in a license key scam. We show this number assigned to

> you. The person on the phone states they are a Microsoft technician to get the victim's registration key. We have a recording of a conversation with one of the potential victims. This number is being disabled on our network.

c. On July 11, 2018, Blitz Telecom emailed Global Voicecom:

> We have been advised that the number 206[XXXXXXX] which we show assigned to your company is being used for fraudulent purposes. This number is being used in false association with Amazon for fraudulent activity....impersonating Amazon to a customer or technical service scam. This number has been reported by Amazon and it has been confirmed the operators are falsely claiming to be Amazon on or around 6/19/18 and 7/10/18.

d. On July 30, 2019, Blitz Telecom emailed Global Voicecom:

> We have been notified that the DID: 502-[XXX]-[XXXX] which we show assigned to Global Voice, are being used in a loan scam. The caller is misrepresenting themselves as being associated with One Main Financial. Due to the fraudulent use of these numbers, they have been disabled on our network. Investigate the use/user of all numbers assigned to this client.

e. On September 26, 2019, Exiant Communications emailed Global Voicecom:

> We have been notified that the DID: 713-[XXX]-[XXXX], which we show assigned to Global Voice, is being used in a Social Security Administration scam. Due to the fraudulent use of this number, it has been disabled on our network. Please investigate other numbers assigned to this client.

f. On September 27, 2019, Exiant Communications emailed Global Voicecom:

> We have received notification that the number 619[XXXXXXX] is being used in connection with a fraudulent IRS/Treasury scam. We show this number assigned to Global Voice. This number has been disabled on our network. Please investigate other numbers assigned to this client.

To virtually all of these warnings and requests for action from Blitz Telecom and Exiant, Global Voicecom would respond that they disabled the phone number that was the subject of the warning.

36. Records from Blitz Telecom show that it provided 902 DID telephone numbers to Defendants Kaen and Global Voicecom. These telephone numbers are used in the fraudulent robocalling schemes as domestic call-back numbers and are contained in the robocall messages. Of the 902 DID telephone numbers provided to Defendants Kaen and Global Voicecom, approximately 493—approximately 55%—are associated with more than 27,000 complaints in the FTC's Consumer Sentinel database. Similarly, YouMail has identified 388 of the 902 DID numbers as being associated with many different fraudulent robocall schemes, including SSA imposters, IRS imposters, USCIS imposters, tech support imposters, loan approval scams, and others. For example:

a. Records from Blitz Telecom show that another DID number it provided to Global Voicecom is 817-[XXX]-[XXXX]. The FTC's Consumer Sentinel database shows 136 complaints involving this telephone number filed between April 18, 2019 and July 23, 2019. Loss data associated with these 136 complaints exceeds $20,000. Records obtained from YouMail, a company that produces robocall-blocking software and which has more than 10 million subscribers, demonstrate that its systems collected information about robocalls involving this telephone number on May 17, 2019 and May 24, 2019, including computer-generated transcripts of the audio. YouMail's systems transcribed the robocall as follows:

> I want you to return the call as soon as possible as SSA has filed a lawsuit against your name the local County Sheriff's are going to arrest you for [ ] serious allegations before this matter goes to the court house and re freeze your bank account and suspend your social security number and get you arrested. For more information regarding this case you can get back to us at 817-[XXX]-[XXXX]. I repeat [XXX]-[XXXX]. Make sure you give us a call back before you get arrested.

b. Similarly, records from Blitz Telecom show that 941-[XXX]-[XXXX] is a DID number it provided to Global Voicecom. The FTC's Consumer Sentinel database shows 190 complaints involving this telephone number filed between September 27, 2018 and November 13, 2019. Loss data associated with these 190 complaints exceeds $34,000. Records obtained from YouMail demonstrate that its systems collected information about robocalls involving this telephone number 26 times between August 2018 and October 2019, including computer-generated transcripts of the audio. YouMail's systems transcribed a September 15, 2018 robocall as follows:

> Hello this is Frankie I'm calling from the Loan Express company here I can see that you had applied for a loan on our company website. So if you are still looking for a loan then your loan amount has been approved for 3000 and the monthly installment off 250 for 16 months. So if you are still interested in this loan then please give us a call back to this number 941-[XXX]-[XXXX]. Thank you.

37. Pursuant to subpoena, Blitz Telecom provided approximately 10 million records of calls involving the 902 DID numbers assigned to Global Voicecom. Analysis of those records show approximately 4.5 million unique phone numbers placing more than 10 million calls to those Global Voicecom DID numbers, which in my experience in this investigation means that approximately 4.5 million different individuals placed (on average) more than one call to those phone numbers. More than 240,000 of these calls were from area codes associated with the Eastern District of New York.

38. Not only do Kaen and his businesses provide DID numbers in service of the fraudulent schemes as call-back numbers, but they also provide toll-free numbers for the same purpose. For example, the FTC received 1,001 SSA-imposter robocalls to their offices on October 23 and 24, 2019. A recording of one of these robocall messages is contained in the audio CD accompanying this Declaration, with the file name *Global Voicecom, et al., SSA Imposter Call to*

FTC October 2019. These robocalls showed as coming from a toll-free telephone number on caller ID, and also contained the same toll-free number in the recorded message as a call-back number. The message is transcribed as follows:

> ...social security on an immediate basis as your social has been found some suspicious for committing fraudulent activities across the United State. Before we go ahead and suspend your social security permanently, we want you to call us back on our department toll free number at 877-[XXX]-[XXXX]. I repeat 8-877-[XXX]-[XXXX]. Do not disregard this message, and call us back as soon as possible. Thank you.

An FTC investigator quickly traced this call to Global Voicecom and Kaen. Toll-free numbers work in a manner similar to DID numbers, but are structured differently by the FCC and telecommunications industry. Somos, Inc. is the FCC-designated national administrator of the U.S. toll-free calling system. Among other functions within the industry, Somos registers "responsible organizations" that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. The FTC investigator contacted Somos, which provided the name of the responsible organization associated with the robocall's toll-free number, and that responsible organization in turn informed the FTC that the number belonged to Kaen and Global Voicecom. In our investigation, we obtained additional records from that responsible organization, including a list of the toll-free numbers it assigned to Kaen and Global Voicecom. These toll-free numbers are associated with approximately 1,400 complaints in the FTC's Consumer Sentinel database.

39. That responsible organization also provided numerous notices to Defendants about how the toll-free numbers assigned to Global Voicecom were being used to commit robocalling fraud, doing so 37 times between March 2019 and October 2019. For example, on April 8, 2019, the responsible organization emailed Defendant Global Voicecom: "We received a scam complaint on the number 888-[XXX]-[XXXX] and were asked to disconnect it. We dialed this number and

found it was someone impersonating Microsoft, and is still connected." Similarly, on June 11, 2019, the responsible organization emailed Defendant Global Voicecom: "Please know that we have rec[ei]ved a serious complaint on TFN 888-[XXX]-[XXXX], which we see i[s] assigned to your account. This number was reported as a part of an "Amazon Customer Support Scam." On August 26, 2019, the responsible organization emailed Defendant Global Voicecom: "Please note that we have received reports that 877-[XXX]-[XXXX] is being used to spoof Bank of America. Can you please look into this, inform us of your results and take action if necessary?" Records provided by the responsible organization show that Kaen and Global Voicecom responded to these warnings, stating that the "offending" number was blocked.

Warnings and Traceback Requests from USTelecom and Company A

40. USTelecom is a nonprofit trade association for the U.S. broadband and communications industry. USTelecom has developed an Industry Traceback Group across the telephonic communications industry to trace robocalls to their sources. In this capacity, USTelecom has identified Defendants' involvement as the initial U.S. point of entry for fraudulent foreign robocalls on numerous occasions, for example:

a. On August 19, 2019, US Telecom emailed Global Voicecom with a traceback request and warning about an August 5, 2019 Social Security Administration impersonation robocall, stating in part:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI is not effective.

The abbreviation ANI stands for "Automatic Number Identification," which in this context refers to the purported source number (the number appearing on the recipient's caller ID). USTelecom was informing Global Voicecom that blocking the specific calling phone number was ineffective as a means of stopping these fraudulent robocalls, because the numbers always can be changed. Nevertheless, the response from Global Voicecom on August 19, 2019 was that it blocked that specific ANI from a source in India, referred to herein as Company A.

b. USTelecom sent a similar notice and another traceback request about a September 2, 2019 SSA imposter robocall to Global Voicecom on September 3, 2019 stating again:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI is not effective.

A recording of the robocall message associated with this USTelecom notice is contained in the audio CD accompanying this Declaration, with the file name *SSA Imposter, September 2, 2019 UST871*. Global Voicecom identified the same Indian source as it did on August 19, 2019, Company A, but this time stated on September 5, 2019 that Global Voicecom took "appropriate action." On September 6, 2019, USTelecom asked what that "action" entailed in light of repeated instances of fraudulent robocalls coming from Global Voicecom and Company A:

> When you state that you have taken appropriate action can you provide detail? [Company A] has been the originator of illegal traffic that is coming through Global Voicecom's network.

Global Voicecom again responded that the action it took was blocking that "offending ANI," i.e., blocking the phone number instead of the person or entity transmitting the fraudulent robocalls.

USTelecom again tried to communicate the futility of such an action, stating on September 6, 2019:

> As stated in our notifications within the workflow, because Caller-ID changes with each call, blocking the ANI is not effective. We can't tell you what to do but we can recommend disconnecting them as a customer or asking for them to stop generating such illegal traffic dealing with government impersonation.

Global Voicecom again responded to the effect that it blocks the specific ANI, and also requests that Company A stop such activity. USTelecom completed tracebacks for 18 fraudulent robocalls traced directly back to Global Voicecom as the gateway carrier between August and November 2019 alone, 16 of which involved Company A as the source of foreign fraudulent robocalls. On nearly every occasion, Global Voicecom would respond to USTelecom's warnings (and others' warnings) with language to the effect that they blocked that particular phone number; however, as was USTelecom's concern about blocking a specific phone number, Global Voicecom did not take action to stop carrying Company A's fraudulent robocalls, for example, by terminating Company A's access to Global Voicecom's systems. Analysis of Paypal records associated with the email address [XXXXXXX]@globalvoicecom.com show that Company A paid Global Voicecom more than $140,000 between 2017 and 2019.

41. Not only has USTelecom sent these notices, warnings, and traceback requests to Global Voicecom, but also to KAT Telecom at the [XXXXXX]75@gmail.com address and another Gmail address used for KAT Telecom. Between May 24, 2019 and January 14, 2020, USTelecom sent approximately two dozen such notices and traceback requests to KAT Telecom, primarily about SSA imposter fraud, as well as IRS imposter fraud, foreign-language imposter fraud, and Amazon imposter fraud. USTelecom was able to complete only a few of the tracebacks,

two of which identified Company A as the source of the fraudulent robocalls and a third that identified another source in India.

42. On May 20, 2019, the FCC subpoenaed Defendants Kaen and Global Voicecom, sending the subpoena to the [XXX]@globalvoicecom.com email address. This subpoena sought production of all records related to a March 26, 2019 fraudulent robocall campaign associated with the spoofed phone number 888-[XXX]-[XXXX], a toll-free number used legitimately by the FCC. YouMail records show that this number is associated with an SSA imposter fraud. On that same day, Global Voicecom responded from the [XXX]@globalvoicecom.com email address, providing records of approximately 13,000 calls placed by one customer on that single day. The response identified the Indian company, Company A, as the foreign source of the thousands of fraudulent robocalls.

Defendants' Foreign Government Consulate Imposter Scheme and Company B

43. On June 19, 2018, the FCC subpoenaed Kaen and his business alias IP Dish, sending the subpoena to Kaen at the [XXXXXX]75@gmail.com email address. This subpoena sought production of records and information related to an "Unlawful Robocall" spoofing the number 212-[XXX]-[XXXX] and placed in February 2018 that the FCC traced back to Kaen and IP Dish. This subpoena was prompted by complaints about robocalls impersonating a foreign-government consulate. Public-domain information reveals that this phone number 212-[XXX-][XXXX] is the local telephone number for a foreign government consulate in New York, New York.

44. In response to the FCC's subpoena, Kaen responded that IP Dish received the call from a foreign entity, referred to herein as Company B. Kaen provided contact information for Company B, including an email address for Company B, [XXXXXXXX]2@gmail.com. In

response to additional questions, Kaen (as "IP Dish NOC") stated that Company B sends tens of thousands of calls per day through IP Dish as a user of VoIP services. Although Kaen represented to the FCC that Company B was a client of IP Dish, records from GoDaddy reveal numerous emails between addresses in the globalvoicecom.com email domain and the [XXXXXXXX]2@gmail.com address. Records from Paypal show that Kaen and Global Voicecom were receiving numerous payments from a Paypal account using the [XXXXXXXX]2@gmail.com address during the first half of 2018, both at the time of the consulate-imposter robocall that was the subject of the FCC subpoena and Kaen's response to the subpoena. Kaen and Global Voicecom continued to do business with the user of the [XXXXXXXX]2@gmail.com address throughout 2018 and 2019, receiving hundreds of payments from the Paypal account using the [XXXXXXXX]2@gmail.com email address, as recently as November 2019; the value of these payments exceeds $140,000.00.

45. As of December 2019, the FTC's Consumer Sentinel database contains 965 complaints about the phone number 212-[XXX]-[XXXX] and the foreign-government consulate robocall scam. These complaints were filed between December 2017 and December 2019. Many of these complaints relate details of the scam, including that the robocall message states that the caller possesses documentation of the called party's illegal immigration status, and that money must be paid to resolve the matter. One of these complaints was filed by L.C., who resides in New York, New York. L.C. states that she was contacted in March, 2018 by the phone number 212-[XXX]-[XXXX] and told that she was a suspect in a money laundering investigation, that fake accounts were opened in her name, that there were numerous victims with large losses, and that she was going to be deported. The scammers created elaborate story lines and were in daily contact

with L.C. for more than two months, during which time she paid them more than $580,000 by wire transfers to banks in Hong Kong.

Data Analysis Related to Defendants' Call Traffic Provides Extensive Evidence of Fraud

46. Analysis of call data obtained in the course of this investigation shows that Kaen's customers' U.S.-bound call traffic consists almost entirely of junk and fraudulent robocalling.

47. In the course of our investigation, we obtained other sets of Kaen's call data records ("CDR"s) related to the robocalling schemes. These data sets include: (1) approximately 7.9 million CDRs obtained from another carrier, TollFreeDeals,[2] for the time period May 20, 2019 – June 11, 2019; and (2) approximately 2.7 million toll-free CDRs obtained from 382 Communications.

48. Analysis of calls Global Voicecom routed through TollFreeDeals reveals that approximately 86% of the calls were shorter than one second, approximately 6.6 million calls, indicating very high levels of junk and fraudulent robocalling, in part arising from calls that do not connect and calls that recipients do not answer. In addition, the approximately 7.9 million calls came from approximately 3.6 million unique source numbers (the numbers appearing on recipients' caller IDs), the vast majority of which were U.S. numbers. Based on my training and experience, there is no legitimate business purpose for which one or several foreign call centers would use millions of different U.S. source numbers to transmit calls to the United States. This massive volume of different source numbers, as well as the ratio of source numbers to calls, is indicative of the use of random, spoofed source numbers in order to: (1) make it appear to potential

---

[2] TollFreeDeals is the DBA name of a defendant in another action filed in this District on the same day as the underlying action in this matter. *United States v. Nicholas Palumbo, et al.* (filed January 27, 2020, E.D.N.Y.).

victims that the calls originate in the United States, and (2) mask from legitimate U.S. carriers and law enforcement the fact that all of these millions of fraudulent calls are originating from the same sources.

49. We then limited the analysis to source numbers with more than 200 calls during the 23-day period to eliminate source numbers with relatively few calls. This limitation revealed 1,899 source numbers that made 3,065,443 calls, ranging from 200 to more than 90,000 calls per source number. 407,881 of those calls were to area codes associated with the Eastern District of New York. Of the 3,065,443 calls, 2,577,436 were shorter than one second, approximately 84%. Again, such a high percentage of short-duration calls indicates very high levels of junk and fraudulent robocalling. Further analysis of these 1,899 source numbers shows that CDRs exist for them, on average, for seven-day periods, ranging from less than one day to a maximum of 22 days. In my training and experience, this short-term usage of phone numbers has no legitimate business use, and indicates that the telephone numbers are discarded once they are turned off due to fraud complaints or are otherwise "burned" by things like robocall-blocking software and complaints to communications carriers.

50. Agents also requested data analysis of the highest-volume source numbers for all traffic passing through TollFreeDeals in that 23-day period, in part to assess how much of that call traffic is fraudulent. According to data maintained by YouMail, of approximately 330,000 calls with five different source numbers sent by Global Voicecom, more than 270,000 (approximately 81%) are associated with known fraudulent robocalling schemes.

Pursuant to 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed on January 27, 2020, in Jamaica, New York.

Sean Fagan
Special Agent
Social Security Administration
Office of the Inspector General